

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

2019 SEP 17 AM 11:40

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)1817 KENTON STREET
SPRINGFIELD, OH 45505
INCLUDING ALL OUTBUILDINGS AND CURTILAGE

Case No.

3:19 mj 559

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

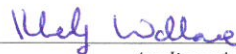
Offense Description

SEE ATTACHMENT C

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA KIMBERLY WALLACE, HSI

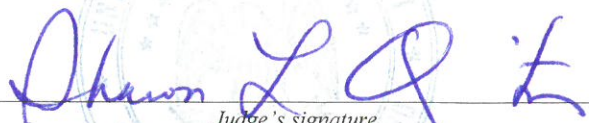
Printed name and title

Sworn to before me and signed in my presence.

Date:

9-17-19

City and state: DAYTON, OHIO



Judge's signature

SHARON L. OVINGTON U.S. MAGISTRATE JUDGE

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at **1817 Kenton St, Springfield, OH 45505**, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The building is a multi-unit, multi-floor, residence bearing two separate numbered addresses with two separate front doors and two separate mailboxes affixed to the building. The numbers “1817” are affixed to the awning, above the porch of the residence, above the door on the left of the residence.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;

ATTACHMENT C

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §§ 2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §§ 2252A(a)(2)(A) & (b)(1)	Receipt or Distribution of Child Pornography
18 U.S.C. §§ 2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §§ 2252(a)(2) & (b)(1)	Receipt or Distribution of Child Pornography
18 U.S.C. §§ 2251(a) and (e)	Production of Child Pornography

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kimberly Wallace, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (“SA”) of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”), since 2010, and am currently assigned to the HSI Resident Agent in Charge Cincinnati, Ohio office. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the location specifically described in **Attachment A** of this Affidavit, including the entire property located at **1817 Kenton St, Springfield, OH** (the “SUBJECT PREMISES”), the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of Title

18, United States Code, Sections 2251, 2252, and 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2251(a) and (e) (production of child pornography); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2251(a) and (e) prohibit any parent, legal guardian, or person having custody or control of a minor who knowingly permits such minor to engage in, or to assist any other person to engage in, sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct shall be punished as provided under subsection (e) of this section, if such parent, legal guardian, or person

knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate

or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. Pursuant to Title 18, United States Code, Section 2256, the term sexually explicit conduct includes the lascivious exhibition of the genitals or pubic area of any person.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Chat group,” as used herein, refers to a group of individuals using an online chat program to communicate electronically in real-time to other individuals in the group in order to send text, pictures, videos, and other content. These chat groups can be public (accessible to everyone using the program) or private (restricted to authorized users). Private chat groups are typically governed by an administrator (or multiple administrators) who have control over who is a member of a particular group.

c. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the

visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISP”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. “Internet Service Providers” or “ISP(s)”, as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. “Mobile application” or “chat application,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

n. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. “Remote computing service”, as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

q. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

r. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON “APPLICATION A”

6. “Application A”¹ is a mobile application designed for chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also

¹ The actual name of “Application A” is known to law enforcement. This chat application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter concerning “Application A,” specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as “Application A.”

has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

7. “Application A” users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, “Application A” users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a “hashtag” that is easily identifiable or searchable by keyword in “Application A.”

PROBABLE CAUSE

8. On or about September 10, 2019, an HSI agent acting in an undercover capacity (hereinafter referred to as UCA), on “Application A”, purported to ^{be known} the father of a minor daughter. ^{SHO}

Pursuant to this investigation, UCA was monitoring a chat group of which user “ct7632” was a member (in “Chat Group 1”²). During the monitoring timeframe, user “ct7632” posted four (4) images of a nude, minor female showering. All images appear to be taken in the same room (the images appear to be surreptitiously taken in a bathroom) based upon the background appearance which showed a window in the background and two loofahs hanging on the wall. Some examples of the shared images include:

² The actual name of “Chat Group 1” is known to law enforcement. This investigation remains active and disclosure of the chat group’s actual name would potentially alert investigative suspects to the fact that law enforcement action is being taken, thereby provoking suspects to notify other users of law enforcement action, flee, and/or destroy evidence.

- a. An image of a nude prepubescent female, from her head to her thighs, facing the camera with her hands raised. Another person's hand is visible in the foreground of the image.
- b. An image of a nude female from behind, showing her buttocks, while another person, wearing an orange shirt, appears to scrub her hair with soap.
- c. An image of a nude female from the side appearing to be taking a shower, based upon the water present in the image. An individual wearing an orange shirt appears on the side of the image.
- d. An image of a nude prepubescent female facing the camera with her hands behind her back. The female appears to be taking a shower while another person, wearing an orange shirt, appears to be rinsing her hair based upon the individual's hand placement on the female's forehead with soap dripping down her front.

9. The UCA sent a private message to user "ct7632" asking the age of the female (in reference to the photographs described in Paragraphs 8a through 8d) to which user "ct7632" responded, "10". The UCA then asked "ct7632" how "ct7632" obtained the images and if they ("ct7632" and the female) were active³ to which "ct7632" responded, "I take all the nudes lol but no we are not active yet. Working on it". "ct7632" also stated, "I take pix every change I get". kw jno

10. Later in "Chat Group 1", user "ct7632" stated, "Just had shower time with my daughter again" and "Now I'm mad tho [sic] lol I had my camera set up and had it pointed to [sic] high" and also made reference to her age and stated, "She is 10".

³ Based upon my training and experience, the term "active" is often utilized to denote involvement or hands-on contact in the sexual abuse of children.

11. User “ct7632” also stated to the UCA, “Just got to watch my sexy daughter take a hot shower and help her. Nothing like watching the soap roll down her body”. The UCA asked “ct7632”, “Do u [sic] shower her every day?” to which “ct7632” replied, “Just about”. The UCA then asked, “Pics [sic] every time?” to which “ct7632” responded, “Ya [sic] pretty much lol”. The UCA asked, “Do u take naughtier pics? Or just showers” to which “ct7632” replied, “Just shower for now. Work in progress”.

12. User “ct7632” also posted in “Chat Group 1”, two (2) non-nude images of a young female who appeared to be the same female referenced in the images described in Paragraphs 8a through 8d.

13. On or about September 10, 2019, an administrative summons was issued to “Application A” for subscriber information for user “ct7632”. A review of the results obtained on or about September 11, 2019 identified a first and last name of “Phillip Na” with a confirmed email address of tyree72590@gmail.com for the account. IP addresses were also listed for the account which reflected IP address 65.29.202.50 being utilized from approximately August 12, 2019 to September 11, 2019.

14. A query of the American Registry for Internet Numbers (“ARIN”) online database revealed that IP address 65.29.202.50 was registered to Charter Communications.

15. On or about September 11, 2019, an emergency disclosure request form was issued to Charter Communications in regard to the IP address described in Paragraph 13. A verbal response (followed by an electronic response the following business day) from Charter Communications, identified the following account holder and address, which is the address of the SUBJECT PREMISES: Leah Cox, **1817 Kenton St, Springfield, OH 45505**.

16. A check with the Ohio Bureau of Motor Vehicles on or about September 11, 2019 revealed that an individual named Charles TYREE with a date of birth of 07/25/1990 resides at the SUBJECT PREMISES.

17. During surveillance conducted of the SUBJECT PREMISES on or about September 16, 2019, a white adult male wearing glasses, matching the description of TYREE (based on Your Affiant's review of various data information systems and open source internet queries), was observed exiting the left front door of the residence, sitting on the porch swing for several minutes before entering the residence through the left front door.

18. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Charles TYREE. These public records indicated that TYREE's current address is SUBJECT PREMISES, **1817 Kenton St, Springfield, OH 45505.**

19. A check of open source information from the Internet regarding Charles TYREE revealed a Facebook account. The profile photograph depicted an adult white male (which matched the driver's license photo for TYREE) sitting on a couch with four minor children. One minor female in the Facebook profile photograph for TYREE matched the photographs posted by user "ct7632" as referenced in Paragraph 12.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

20. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers

basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a

digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*,

temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, DISTRIBUTE, AND/OR POSSESS CHILD PORNOGRAPHY

21. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, distribute, and/or possess child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Such individuals almost always possess and maintain their hard copies of

child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child

pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Charles TYREE uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A.

22. Based on the following, I believe that the user of “ct7632” residing at the SUBJECT PREMISES likely displays characteristics common to individuals who produce, distribute, and possess child pornography. For example, the target of this investigation posted the below comment:

- a. User “ct7632” posted a comment in “Chat Group 1” that stated, “Finally not dealing with only collectors haha”.⁴

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

⁴ Based on my training and experience, and given my knowledge of the investigation, it appears that “ct7632” believed that he was in a chat group focused on producers of child pornography, as opposed to a chat group focused on collectors of child pornography.

23. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

25. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal

information such as online usernames, nicknames, and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP

addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of

Internet discussions about the crime; and other records that indicate the nature of the offense.

26. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or

alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.


27. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

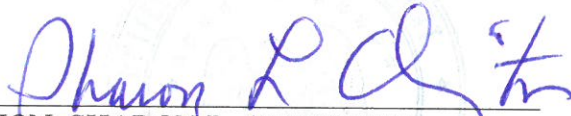
29. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and (e) (production of child pornography); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), as described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.


30. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



Kimberly Wallace
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 17th day of September 2019.


HON. SHARON L. OVINGTON
UNITED STATES MAGISTRATE COURT JUDGE



ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at **1817 Kenton St, Springfield, OH 45505**, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The building is a multi-unit, multi-floor, residence bearing two separate numbered addresses with two separate front doors and two separate mailboxes affixed to the building. The numbers “1817” are affixed to the awning, above the porch of the residence, above the door on the left of the residence.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography, as defined in 18 U.S.C. § 2256(8), and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:

- a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, **1817 Kenton St, Springfield, OH 45505**, including utility and telephone bills, mail envelopes, or addressed correspondence;
- b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
- d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of the website referenced in the Search Warrant Application;
- e. Records and information showing access to and/or use of the website referenced in the Search Warrant Application; and
- f. Records and information relating or pertaining to the identity of the person or persons using or associated with ct7632 and/or Phillip Na.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.